SYLVESTER'S FORM OF THE RESULTANT AND THE MATRIX-TRIANGULARIZATION SUBRESULTANT PRS METHOD

ALKIVIADIS G. AKRITAS*

Summary. Sylvester's form of the resultant is often encountered in the literature but is completely different from the one discussed in this paper; the form described here can be found in Sylvester's paper of 1853 [12], and has been previously used only once, by Van Vleck [13] in the last century. Triangularizing this "rediscovered" form of the resultant we obtain a new method for computing a greatest common divisor (gcd) of two polynomials in $\mathbf{Z}[x]$, along with their polynomial remainder sequence (prs); since we are interested in exact integer arithmetic computations we make use of Bareiss's [4] integer-preserving transformation algorithm for Gaussian elimination. This new method uniformly treats both complete and incomplete prs's and, for the polynomials of the prs's, it provides the smallest coefficients that can be expected *without* coefficient gcd computations.

1. Introduction. In this note we restrict our discussion to univariate polynomials with integer coefficients and to computations in $\mathbf{Z}[x]$, a unique factorization domain. Given the polynomial $p(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_0$, its degree is denoted by $\deg(p(x))$ and c_n, its leading coefficient, by $lc(p)$; moreover, $p(x)$ is called *primitive* it its coefficients are relatively prime.

Consider now $p_1(x)$ and $p_2(x)$, two primitive, nonzero polynomials in $\mathbf{Z}[x]$, $\deg(p_1(x)) = n$ and $\deg(p_2(x)) = m$, $n \geq m$. Clearly, the polynomial division (with remainder) algorithm, call it **PD**, that works over a field, cannot be used in $\mathbf{Z}[x]$ since it requires exact divisibility by $lc(p_2)$. So we use *pseudo-division*, which always yields a pseudo-quotient and pseudo-remainder; in this process we have to premultiply $p_1(x)$ by $lc(p_2)^{n-m+1}$ and then apply algorithm PD. Therefore we have:

$$(1) \qquad lc(p_2)^{n-m+1}p_1(x) = q(x)p_2(x) + p_3(x), \quad \deg(p_3(x)) < \deg(p_2(x)).$$

Applying the same process to $p_2(x)$ and $p_3(x)$, and then to $p_3(x)$ and $p_4(x)$, etc. (Euclid's algorithm), we obtain a *polynomial remainder sequence* (prs)

$$p_1(x), p_2(x), p_3(x), \ldots p_h(x), p_{h+1}(x) = 0,$$

where $p_h(x) \neq 0$ is a greatest common divisor of $p_1(x)$ and $p_2(x)$, $gcd(p_1(x), p_2(x))$. If $n_i = \deg(p_i(x))$ and we have $n_i - n_{i+1} = 1$, for all i, the prs is called *complete*, otherwise, it is called *incomplete*. The problem with the above approach is that the coefficients of the polynomials in the prs grow exponentially and hence slow

*University of Kansas, Department of Computer Science, Lawrence, Kansas 66045 down the computations. We wish to control this coefficient growth. We observe that equation (1) can also be written more generally as

$$(2) \quad lc(p_{i+1})^{n_i - n_{i+1} + 1} p_i(x) = q_i(x) p_{i+1}(x) + \beta_i p_{i+2}(x), \quad \deg(p_{i+2}(x)) < \deg(p_{i+1}(x)),$$

$i = 1, 2, \ldots, h-1$. That is, if a method for choosing β_i is given, the above equation provides an algorithm for constructing a prs. The obvious choice $\beta_i = 1$, for all i, is called the *Euclidean prs*; it was described above and leads to exponential growth of coefficients. Choosing β_i to be the greatest common divisor of the coefficients of $p_{i+2}(x)$ results in the *primitive prs*, and it is the best that can be done to control the coefficient growth. (Notice that here we are dividing $p_{i+2}(x)$ by the greatest common divisor of its coefficients before we use it again). However, computing the greatest common divisor of the coefficients for each member of the prs (after the first two, of course) is an expensive operation and should be avoided. So far, in order to control the coefficient growth and to avoid the coefficient gcd computations, either the *reduced* or the (improved) *subresultant* prs have been used. In the reduced prs we choose

$$(3) \qquad \beta_1 = 1 \quad \text{and} \quad \beta_i = lc(p_i)^{n_{i-1} - n_i + 1}, \quad i = 2, 3, \ldots, h-1,$$

whereas, in the subresultant prs we have

$$(4) \quad \beta_1 = (-1)^{n_1 - n_2 + 1} \quad \text{and} \quad \beta_i = (-1)^{n_i - n_{i+1} + 1} lc(p_i) H_i^{n_i - n_{i+1}}, \quad i = 2, 3, \ldots, h-1,$$

where

$$H_2 = lc(p_2)^{n_1 - n_2} \quad \text{and} \quad H_i = lc(p_i)^{n_{i-1} - n_i} H_{i-1}^{1 - (n_{i-1} - n_i)}, \quad i = 3, 4, \ldots, h-1.$$

That is, in both cases above we divide $p_{i+2}(x)$ by the corresponding β_i before we use it again. The reduced prs algorithm is recommended if the prs is complete, whereas if the prs is incomplete the subresultant prs algorithm is to be preferred. The proofs that the β_i's shown in (3) and (4) exactly divide $p_{i+2}(x)$ are very complicated [7] and have up to now obscured simple divisibility properties [11], (see also [5] and [6]). For a simple proof of the validity of the reduced prs see [1]; analogous proof for the subresultant prs can be found in [8].

In contrast with the above prs algorithms, the matrix-triangularization subresultant prs method avoids explicit polynomial divisions. In what follows we present this method. We also present an example where bubble pivot is needed.

2. Sylvester's form of the resultant. Consider the two polynomials in $Z[x]$, $p(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0$ and $p_2(x) = d_m x^m + d_{m-1} x^{m-1} + \cdots + d_0$, $c_n \neq 0$, $d_m \neq 0$, $n \geq m$. In the literature the most commonly encountered forms of the resultant of $p_1(x)$ and $p_2(x)$ (both known as "Sylvester's" forms) are:

$$\operatorname{res}_B(p_1,p_2)=\begin{vmatrix} c_n & c_{n-1} & \cdots & & c_0 & 0 & \cdots & 0 \\ 0 & c_n & c_{n-1} & \cdots & & c_0 & \cdots & 0 \\ & & & & & \vdots & & \\ 0 & 0 & \cdots & & c_n & c_{n-1} & \cdots & c_0 \\ d_m & d_{m-1} & \cdots & d_0 & 0 & 0 & \cdots & 0 \\ 0 & d_m & d_{m-1} & \cdots & d_0 & 0 & \cdots & 0 \\ & & & & \vdots & & & \\ 0 & 0 & \cdots & d_m & d_{m-1} & & \cdots & d_0 \end{vmatrix}$$

or

$$\operatorname{res}_T(p_1,p_2)=\begin{vmatrix} c_n & c_{n-1} & \cdots & & c_0 & 0 & \cdots & 0 \\ 0 & c_n & c_{n-1} & \cdots & & c_0 & \cdots & 0 \\ & & & & & \vdots & & \\ 0 & 0 & \cdots & & c_n & c_{n-1} & \cdots & c_0 \\ 0 & 0 & \cdots & d_m & d_{m-1} & & \cdots & d_0 \\ & & & & \vdots & & & \\ 0 & d_m & d_{m-1} & \cdots & d_0 & 0 & \cdots & 0 \\ d_m & d_{m-1} & \cdots & d_0 & 0 & 0 & \cdots & 0 \end{vmatrix}$$

where for both cases we have m rows of c's and n rows of d's; that is, the determinant is of order $m+n$. Contrary to established practice, we call the first Bruno's and the second Trudi's form of the resultant [3]. Notice that $\operatorname{res}_B(p_1,p_2) = (-1)^{n(n-1)/2}\operatorname{res}_T(p,p_2)$. We choose to call Sylvester's form the one described below; this form was "buried" in Sylvester's 1853 paper [12]and is only once mentioned in the literature in a paper by Van Vleck [13]. Sylvester indicates ([12]), p. 426 that he had produced this form in 1839 or 1840 and some years later Cayley unconsciously reproduced it as well. It is Sylvester's form of the resultant that forms the foundation of our new method for computing polynomial remainder sequences; however ,we first present the following theorem concerning Bruno's form of the resultant:

THEOREM 1 (Laidacker [10]). *If we transform the matrix corresponding to* $\operatorname{res}_B(p_1(x),p_2(x))$ *into its upper triangular form* $T_B(R)$, *using row transformations only, then the last nonzero row of* $T_B(R)$ *gives the coefficients of a greatest common divisor of* $p_1(x)$ *and* $p_2(x)$.

The above theorem indicates that we can obtain only a greatest common divisor of $p_1(x)$ and $p_2(x)$ but none of the remainder polynomials. In order to compute both a $gcd(p_1(x), p_2(x))$ and all the polynomial remainders we have to use Sylvester's form of the resultant; this is of order $2n$ (as opposed to $n + m$ for the other forms) and of the following form ($p_2(x)$ has been transformed into a polynomial of degree n by introducing zero coefficients):

$$\text{res}_S(p, q) = \begin{vmatrix} c_n & c_{n-1} & \dots & c_0 & 0 & 0\dots0 \\ d_n & d_{n-1} & \dots & d_0 & 0 & 0\dots0 \\ 0 & c_n & \dots & c_0 & 0\dots0 & \\ 0 & d_n & \dots & d_0 & 0\dots0 & \\ & & \dots\dots\dots & & & \\ 0 & \dots & 0 & c_n & c_{n-1} & \dots & c_0 \\ 0 & \dots & 0 & d_n & d_{n-1} & \dots & d_0 \end{vmatrix} \qquad (S)$$

Sylvester obtains this form from the system of equations ([12]) pp. 427–428)

$$\begin{gathered} p(x) = 0 \\ q(x) = 0 \\ x \cdot p(x) = 0 \\ x \cdot q(x) = 0 \\ x^2 \cdot p(x) = 0 \\ x^2 \cdot q(x) = 0 \\ \dots\dots \\ x^{n-1} \cdot p(x) = 0 \\ x^{n-1} \cdot q(x) = 0 \end{gathered}$$

and he indicates that if we take k pairs of the above equations, the highest power of x appearing in any of them will be x^{n+k-1}. Therefore, we shall be able to eliminate so many powers of x, that x^{n-k} will be the highest power uneliminated and $n-k$ will be the degree of a member of the Sturmian polynomial remainder sequence generated by $p(x)$ and $q(x)$. Moreover, Sylvester showed that the polynomial remainders thus obtained are what he terms *simplified residues*; that is, the coefficients are the smallest possible obtained without integer *gcd* computations and without introducing rationals. Stated in other words, the polynomial remainders have been freed from their corresponding *allotrious factors*.

It has been proved [13] that if we want to compute the polynomial remainder sequence $p_1(x)$, $p_2(x)$, $p_3(x), \dots, p_h(x)$, $\deg(p_1(x)) = n$, $\deg(p_2(x)) = m$, $n \geq m$, we can obtain the (negated) coefficients of the $(i + 1)$th member of the *prs*, $i = 0, 1, 2, \dots,\ h - 1$, as minors formed from the first 2i rows of (S) by successively associating with the first 2i-1 columns (of the (2i) by (2n) matrix) each succeeding column in turn.

Instead of proceeding as above, we transform the matrix corresponding to the resultant (S) into its upper triangular form and obtain the members of the prs with

the help of Theorem 2 below. We also use Bareiss's integer-preserving transformation algorithm [4]; that is:
let $r_{00}^{(-1)} = 1$, and $r_{ij}^{(0)} = r_{ij}$, $i, j = 1, \ldots, n$; then for $k < i, j \leq n$,

$$r_{ij}^{(k)} := (1/r_{k-1,k-1}^{(k-2)}) \cdot \begin{vmatrix} r_{kk}^{(k-1)} & r_{kj}^{(k-1)} \\ r_{ik}^{(k-1)} & r_{ij}^{(k-1)} \end{vmatrix} \tag{5}$$

Of particular importance in Bareiss's algorithm is the fact that the determinant of order 2 is divided *exactly* by $r_{k-1,k-1}^{(k-2)}$ (the proof is very short and clear and is described in Bareiss's paper [4]) and that the resulting coefficients are the smallest that can be expected without coefficient *gcd* computations and without introducing rationals. Notice how all the complicated expressions for β_i in the reduced and subresultant *prs* algorithms are mapped to the simple factor $r_{k-1,k-1}^{(k-2)}$ of this method.

It should be pointed out that using Bareiss's algorithm we will have to perform pivots (interchange two rows) which will result in a change of signs. We also define the term *bubble* pivot as follows: if the diagonal element in row i is zero and the next nonzero element down the column is in row $i + j$, $j > 1$, then row $i + j$ will become row i after pairwise interchanging it with the rows above it. Bubble pivot preserves the symmetry of the determinant.

We have the following theorem.

THEOREM 2 ([2]). *Let $p_1(x)$ and $p_2(x)$ be two polynomials of degrees n and m respectively, $n \geq m$. Using Bareiss's algorithm transform the matrix corresponding to $\text{res}_S(p_1(x), p_2(x))$ into its upper triangular form $T_S(R)$; let n_i be the degree of the polynomial corresponding to the i-th row of $T_S(R)$, $i = 1, 2, \ldots, 2n$, and let $p_k(x), k \geq 2$, be the kth member of the (complete or incomplete) polynomial remainder sequence of $p_1(x)$ and $p_2(x)$. Then if $p_k(x)$ is in row i of $T_S(R)$, the coefficients of $p_{k+1}(x)$ (within sign) are obtained from row $i + j$ of $T_S(R)$, where j is the smallest integer such that $n_{i+j} < n_i$. (If $n = m$ associate both $p_1(x)$ and $p_2(x)$ with the first row of $T_S(R)$.)*

We see, therefore, that based on Theorem 2, we have a new method to compute the polynomial remainder sequence and a greatest common divisor of two polynomials. This new method uniformly treats both complete and incomplete *prs*'s and provides the smallest coefficients that can be expected without coefficient *gcd* computation.

3. The matrix-triangularization subresultant prs method. The inputs are two (primitive) polynomials in $\mathbf{Z}[x]$, $p_1(x) = c_n x^n + c_{n-1} + \cdots + c_0$ and $p_2(x) = d_m x^m + d_{m-1} x^{m-1} + \cdots + d_0$, $c_n \neq 0$, $d_m \neq 0$, $n \geq m$.

Step 1: Form the resultant (S), $\text{res}_S(p_1(x), p_2(x))$, of the two polynomials $p_1(x)$ and $p_2(x)$.

Step 2: Using Bareiss's algorithm (and bubble pivot) transform the resultant (S) into its upper triangular form $T_S(R)$; then the coefficients of all the members of the polynomial remainder sequence of $p_1(x)$ and $p_2(x)$ are obtained from the rows of $T_S(R)$ with the help of Theorem 2.

For this method we have proved [2] that its computing time is:

THEOREM 3. *Let* $p_1(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_0$ *and* $p_2(x) = d_m x^m + d_{m-1}x^{m-1} + \cdots + d_0$, $c_n \neq 0$, $d_m \neq 0$, $n \geq m$ *be two (primitive) polynomials in* $\mathbf{Z}[x]$ *and for some polynomial* $P(x)$ *in* $\mathbf{Z}[x]$ *let* $|P|_\infty$ *represent its maximum coefficient in absolute value. Then the method described above computes a greatest common divisor of* $p_1(x)$ *and* $p_2(x)$ *along with all the polynomial remainders in time*

$$0(n^5 L(|p|_\infty)^2)$$

where $|p|_\infty = \max(|p_1|_\infty), |p_2|_\infty)$.

Below we present an incomplete example where bubble pivoting is needed [3]; note that there is a difference of 3 in the degrees of the members of the *prs*, as opposed to a difference of 2 in Knuth's "classic" incomplete example [2].

Example. Let us find the polynomial remainder sequence of the polynomials $p_1(x) = 3x^9 + 5x^8 + 7x^7 - 3x^6 - 5x^5 - 7x^4 + 3x^3 + 5x^2 + 7x - 2$ and $p_2(x) = x^8 - x^5 - x^2 - x - 1$. This incomplete *prs* example presents a variation of three in the degrees of its members (from 7 to 4) and it requires a bubble pivot in the matrix-triangularization method; that is, the special kind of pivot described above will take place between rows that are not adjacent (the pivoted rows are marked by "#").

The matrix-triangularization subresultant prs method

row		degree
1 >	3 5 7 −3 −7 3 5 7 −2 0 0 0 0 0 0 0 0	(9)
2 >	0 1 0 0 −1 0 0 −1 −1 −1 0 0 0 0 0 0 0 0	(8)
3)	0 0 5 7 0 −5 −7 6 8 10 −2 0 0 0 0 0 0 0	(8)
4 >	0 0 0 −7 0 0 7 −6 −13 −15 −3 0 0 0 0 0 0 0	(7)
5)	0 0 0 0 −49 0 0 79 23 19 −55 14 0 0 0 0 0 0	(7)
#6)	0 0 0 0 0 −343 0 −24 501 73 93 −413 98 0 0 0 0 0	(7)
#7)	0 0 0 0 0 0 −2401 −510 −1273 1637 −339 56 −2891 686 0 0 0 0	(7)
8 >	0 0 0 0 0 0 0 2058 4459 7546 3430 2401 0 0 0 0 0 0	(4)
9)	0 0 0 0 0 0 0 0 −1764 −3822 −6468 −2940 −2058 0 0 0 0 0	(4)
10)	0 0 0 0 0 0 0 0 0 1512 3276 5544 2520 1764 0 0 0 0	(4)
11)	0 0 0 0 0 0 0 0 0 0 25811 −18982 4520 −811 −3024 0 0 0	(4)
12 >	0 0 0 0 0 0 0 0 0 0 0 −64205 −77246 −37568 −28403 0 0 0	(3)
13)	0 0 0 0 0 0 0 0 0 0 0 0 2124693 449379 519299 128410 0 0	(3)
14 >	0 0 0 0 0 0 0 0 0 0 0 0 0 −5240853 −1800739 −2018639 0 0	(2)
15)	0 0 0 0 0 0 0 0 0 0 0 0 0 0 −22909248 −24412716 10481706 0	(2)
16 >	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 −40801132 47620330 0	(1)
17)	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 −398219984 81602264	(1)
18 >	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 682427564	(0)

The members of the prs are obtained from the rows whose numbers are followed by ">", except for row 8 in which case the smaller coefficients shown below, in 6 >, are taken as the coefficients of the polynomial. The largest integer generated is 27343817119202448 [17 digits].

Pivoted row 6 during transformation 6. Stored row is:

```
6 >      0 0 0 0 0 0 0 42 91 154 70 49 0 0 0 0 0 0
```

Pivoted row 7 during transformation 7. Stored is:

```
7)      0 0 0 0 0 0 0 294 637 1078 490 343 0 0 0 0 0 0
```

REFERENCES

[1] AKRITAS, A.G., *A simple validity proof of the reduced prs algorithm*, Computing 38 (1987), 369–372.

[2] AKRITAS, A.G., *A new method for computing greatest common divisors and polynomials remainder sequences*, Numerische Mathematik 52 (1988), 119–127.

[3] AKRITAS, A.G., *Elements of Computer Algebra with Applications*, John Wiley Interscience, New York, 1989.

[4] BAREISS, E.H., *Sylvester's identity and multistep integer-preserving Gaussian elimination*, Mathematics of Computation 22 (1968), 565–578.

[5] BROWN, W.S., *On Euclid's algorithm and the computation of polynomial greatest common divisors*, JACM 18, (1971) 476–504.

[6] BROWN, W.S., *The subresultant prs algorithm*, ACM Transactions On Mathematical Software 4 (1978), 237–249.

[7] COLLINS, G.E., *Subresultants and reduced polynomial remainder sequences*, JACM 14 (1967), 128–142.

[8] HABICHT, W., *Eine Verallgemeinerung des Sturmschen Wurzelzaehlverfahrens*, Commentarii Mathematici Helvetici 21 (1948), 99–116.

[9] KNUTH, D.E., *The art of computer Programming*, Vol. II, 2nd ed.: Seminumeral Algorithms. Addison-Wesley. Reading MA, 1981.

[10] LAIDACKER, M.A., *Another theorem relating Sylvester's matrix and the greatest common divisor*, Mathematics Magazine 42 (1969), 126–128.

[11] LOOS, R., *Generalized polynomial remainder sequences*. In: Computer Algebra Symbolic and Algebraic Computations. Ed. by B. Buchberger, G.E. Collins and R. Loos, Springer Verlag, Wien, New York, 1982, Computing Supplement 4, 115–137.

[12] SYLVESTER, J.J., *On a theory of the syzegetic relations of two rational integral functions, comprising an application to the theory of Sturm's functions, and that of the greatest algebraical common measure*, Philosophical Transactions 143 (1853), 407–584.

[13] VAN VLECK, E.B., *On the determination of a series of Sturm's functions by the calculation of a single determinant*, Annals of Mathematics, Second Series, Vol. 1, (1899–1900) 1–13.